State of the Net - February 12 2024

36 Fireside Chat with Under Secretary Robert Silvers

Shane Tews - President, Logan Circle Strategies
The Honorable Robert Silvers - Under Secretary for Policy, Department of Homeland Security

Shane Tews
I'm Shane Tews. I am the board director. I've been excited to be part of this program for a really long time. But, I'm even more excited to introduce the Undersecretary of the Department of Homeland Security, Rob Silver. He has been the undersecretary for this administration, but he was also previously with the Obama administration, and he's had an extensive career focused on cybersecurity, which we couldn't say 20 years ago when we were doing this. So, it's so exciting to have someone that's really been in the trenches, and has been teaching this also from a legal perspective. He has been part of a prominent public partnership in the legal sector, and he's now rejoined DHS.

But, before we delve into cybersecurity challenges, I want to rewind a little bit, and could you share us some of the insights from your previous role as the Assistant Secretary of Cyber Policy and Deputy Chief of Staff at DHS? So, you've had a tremendously large role at the agency twice?

Robert Silvers
Yes, those were positions I held in the Obama administration, and it it truly is an incredibly broad and sprawling department, the Department of Homeland Security. The missions range from the tech security issues that we talk about here, AI safety, cybersecurity, and the like, but then they run to disaster response, counterterrorism, a range of law enforcement issues, the border, we have the Secret Service, the Coast Guard, TSA, and on and on, and so it's an incredibly powerful department in terms of the range of tools we have, and that can that we can bring to take on the heaviest challenges that we face from a security and safety perspective.

Shane Tews
And now, a lot of the Biden administration's Executive Order on artificial intelligence falls on your shoulders, so you have a tremendous amount of what's going on in that space. So, talk to us about how... Are you making everyone in the agency an AI expert? I mean, how do you tackle that?

Robert Silvers
Yeah, I think that everybody, no matter what their job, should obtain a certain level of literacy and proficiency with artificial intelligence technology, at least as a consumer and user of it, because it's going to be so ubiquitous. What we are very focused on is developing and growing a team of AI safety and security experts. I do want to just say at the outset that at a lot of events, you get into a really doom and gloom vibe of people talking about all the terrible things that are going to happen because of artificial intelligence, and I don't believe in that kind of conversation. Artificial Intelligence is going to cure cancer and other diseases, it's going to level up economic opportunities for those that didn't have every advantage growing up, and so much more. At the department, we are using artificial intelligence technology now to better detect fentanyl shipments, to advance screening at the airport so it's more efficient and customer friendly, and the like.

The challenge is to embrace all this technology and harness its benefits, but in a way that's protective, and really to build an architecture of security and safety for it to grow on top of. That's what we're focused on. The Executive Order that President Biden signed last year on artificial intelligence put the Department of Homeland Security on point for driving safe and secure adoption of artificial intelligence in a number of respects. First, with respect to critical infrastructure, you think about hospital systems, the power grid, financial markets. As operators of critical infrastructure deploy AI technology into their their operations, we want to make sure that it's done safely, that when things fail, it fails safely not catastrophically, that it's protected from attack, or from accidents, that can cause real physical world consequences. And so, we are going to be developing guidance for critical infrastructure companies, as well as AI model developers, on

how to build safety and security into their products and into their systems. We're very focused. Another part of the executive order tasked us with making sure we are reducing risks with respect to bio-warfare, because artificial intelligence can potentially be used to develop new synthetic biological weapons and the like. And so, we're taking all of this on, but again, not with a goal of tamping down the technology, or saying that it isn't something we should do, we absolutely should lean in hard on embracing the technology, but again, doing it safely and securely.

Shane Tews
I hear you on the techno-optimism, and I'm with you, I think it's going to do amazing things. You just recently returned from China. We're supposed to be in a race with them. Are you concerned that we're going to be in some sort of head-to-head, and China gets there first, to get to make the rules, or are we the ones that need to decide, from a democratic perspective, how artificial intelligence is used? That seems to be kind of the current thought process that's going on in this town, at least in a lot of the discussions around artificial intelligence, well, globally.

Robert Silvers
It's definitely competitive between the United States and China right now. The tech race is one primary arena in which their competition is playing out, and I do think that US companies are ahead when it comes to artificial intelligence, but it's not the kind of lead where you can grow complacent. There's going to be competition into who can develop the most advanced products. I think we need to be mindful as we make our policies, and take actions as a government, to make sure we are fostering a very strong and agile artificial intelligence ecosystem here in the United States. There's going to be governance decisions that have to be made, where governments need to think through how are we going to set rules of the road. China has introduced certain AI regulations, so has Europe, for that matter, and so that's going to be a part of this, as well.

Shane Tews
And, a lot is the discussion around guardrails, and that's been very interesting. We've seen the EU AI Act, OECD has had several working groups on that. I still don't understand why UNESCO has things going on, but they do. But, going more to cyber, the kind of dual side of this, it's going to make the ability to watch and thwart and enable a better defense on attacks, but it also will enable our attackers to be just as smart, if not smarter. So, how do we get prepared for the balance, where we need to know both sides of that equation?

Robert Silvers
There's just no question that that artificial intelligence, in its simplest terms, is just like any other kind of invention, where it can be used for good or for bad. The same can be said of the invention

of the knife, or the invention of fire. There's all kinds of offensive or adversarial use cases for AI that certainly are cause for concern, and that we need to be super vigilant towards. There's also really powerful defensive applications. The jury is still out as to who it will benefit more, offense or defense. I think it'll be a mixed landscape, there's going to be powerful benefits for both sets of actors. I will say that, from what we see happening in the wild right now, I see a lot more promising defensive use of AI actually happening, in corporate environments or government environments, than I see actual adversarial use of AI to inflict harm, but that's a snapshot. That's right now.

Certainly, bad actors are experimenting with AI to see what they can do, to use it to amplify what they want to do, or scale up what they want to do. We're seeing fraud tools that are fueled by large language models, that can sort of help create business email compromise and phishing, and other kinds of spammy or fraudulent messages and emails that appear more realistic and can be sent out at scale. We're certainly seeing experimentation with artificial intelligence technology to develop deep fakes and other kinds of disinformation flows by nation state actors that want to destabilize our system here. So, I don't mean to dismiss it, it's a really serious thing. But, again, on the defensive side, artificial intelligence has been used in the cybersecurity industry for a long time, and that use will only increase. It's really powerful for detect thing anomalous activity in a very busy and noisy network environment. So, I think I think this will just play out, and I think there's going to be wins for the offense and the defense over time.

Shane Tews
So, I'm thinking both the Department and the commercial market. The Sony hack was a big wake up call about things that you do, and the the use of human intelligence on how we could attack the networks. Then we had the Colonial Pipeline, just because it was so incredibly involved in what they were doing. Human intelligence was exceptionally important. I loved how many FBI agents got hired as CISOs and CTOs after that. It was like, all of a sudden, we got to protect this stuff. Do we need to have another challenging incident like that? Are people really preparing, both in the government and in the commercial market, for what is probably lying ahead with artificial intelligence? I worry that some of these people are just sitting ducks.

Robert Silvers
We're not where we want to be on cybersecurity,, as a country as a whole. But, I think if you look at where organizations are now, versus 3 years ago, 5 years ago, 10 years ago, they are generally more hardened up. The cat and mouse still continues. As organizations harden up, the threat actors find new and innovative ways to challenge their defenses, so that still goes on. But, it's not

hopeless. In fact, there's a lot of cause for hope, that if an organization does make the necessary investment, it will be able to protect itself.

Two years ago or so, when Russian forces were massing on the Ukrainian border, and it became clear that an invasion could be imminent, the Ukrainian government made a very wise set of decisions. They decided to immediately surge investment into protecting their digital infrastructure. They moved a lot of their systems and data to the cloud, so that it wasn't resident in data centers in Ukraine. They brought in Western companies like Microsoft and Mandiant, and others, to help them get ready from a network defense perspective. They worked closely with US government and other allied country cybersecurity agencies to help them get ready. What you ended up seeing, when the invasion began, was that the Ukrainians succeeded in defending and repelling way more Russian cyber attacks than anyone thought possible. Some attacks landed, but the the defense actually worked. And now, if Russia wants to take out the grid in Ukraine, they launch a missile and they don't really do a cyber attack, and missiles are expensive and scarce for them. It shows that defense matters. Resilience matters. if you put in the time, and the effort, and the resources, and the human capital, to achieving it. That's the takeaway.

Shane Tews
It's been fascinating to read how much technology has been in Ukraine. At the very beginning, they were very open to anybody, take all comers, and then they're like, wait a minute, we need to maybe get a little more organized and thoughtful about this, because they just had so many people showing up in their country to start deploying things, and they didn't really know exactly what everybody was up to. So, that was kind of fascinating.

Going forward, on just artificial intelligence -- we can step away from cyber directly -- what is it that excites you about it? What is it that you've seen that you're, like, I cannot wait for this to take hold, and this to be the norm.

Robert Silvers
People being able to put their more routine tasks to the side, and use their time more efficiently, and for higher and better uses, is exciting. There's a lot of opportunity to level the playing field for people that didn't have a lot of advantages in their upbringing, or their educational opportunities. Think about it like a resume. There's probably a lot of people in this room who know how to write a resume, but, for a lot of people, they didn't grow up in a household or a school where they had anybody to teach them how to do that. Now, using chat bots and other AI-powered technologies, you can get a pretty cool looking resume put together really really fast, and present yourself as somebody who knows how to do that. I view that as a field leveling opportunity. When the iPhone

was invented, I don't even think Steve Jobs could have predicted this app or that app that would ultimately make it onto the App Store years later, but it created a platform to do things like that, and for other people to take their creativity, and use the invention to do incredible things. It's going to totally be the same. I think, with AI. It's not going to need to be the big frontier model companies that need to think of everything, others will be able to take it, and just do incredible things. And so, I really look forward to seeing what everybody comes up with.

Shane Tews
I was saying earlier to somebody who's a teacher, I'd like to see the questions that the kids are asking it. They're probably a lot more creative than the things, because we're already in our little rote memory cycles.

Okay, it's almost five o'clock. Do you mind taking just a couple questions? Okay. All right. We're gonna do, like, two and then we're going to get out of here. Right here. Over here. David, introduce yourself.

David DiMolfetta
Hi, I'm David DiMolfetta, I cover cybersecurity for NextGovFCW. We just reported that GAO was notified of a breach, do you have a response to that?

Robert Silvers
I don't have anything to add on that.

David DiMolfetta
Cool. Thank you.

(Audience)
[Laughter]

Shane Tews
Good reporting. Well done. Right, over here. Yeah.

Derek Wyatt
I'm Derek Wyatt, a former MP in England. When you created the 14 points from Woodrow Wilson, and one of them was the League of Nations, you didn't join. So, if you're now saying that you are going to join some kind of world AI body, are you really going to do it?

Robert Silvers
Well, we're really actively engaging in a number of multilateral fora, where like minded countries are coming together to figure out the governance and the rules of the road around this powerful technology, and that includes direct dialogues with the UK and with the EU, and others as well. We were contributors and participants in the UK AI safety summit that took place last year. I think it's an open question, what global governance, if any, of this technology will actually look like, and I think we ought to be kind of humble in getting too specific about what it should look like, at this point, because I'm not sure that we have a monopoly on the good ideas, yet, of the twists and turns this can take, and so I think what we're doing is we are taking a balanced and protective approach of identifying guardrails that ought to be included in these systems, encouraging voluntary commitments by the leading companies, such as those that the White House rolled out together with companies late last year, and then participating in all these global fora to make sure that we're doing the right things with like minded allies and partners.

I will say, another important initiative of the Biden administration, as part of its commitment to AI safety and security, is our department was charged in the Executive Order with creating an Artificial Intelligence Safety and Security Board, and it's modeled on the Cyber Safety Review Board that we created in 2021, and which has proven very successful. The Secretary of Homeland Security is going to personally chair this board, and it is going to have representatives from leading companies, academia, NGOs, civil society, privacy and civil liberties advocates, and the like, a range of views, to jointly come together and make actionable recommendations for how companies, governments, and other stakeholders, can increase safety and security when it comes to artificial intelligence. That's a really important model, because I don't think you can have government going it alone on this issue, just for a whole host of reasons. This is going to be a truly public-private initiative, where some of the members are all the federal leads, not just from DHS, for AI safety and security, and other members come from different segments of our society, corporate America and civil society and the like, to bring all the views together and try to align on very specific actionable approaches to make sure that, as we adopt these technologies, it's done in a safe and secure way.

Shane Tews
Last question, right here.

Alex Howard
Alex Howard. Thanks for mentioning the use case of fentanyl. I didn't see that in the AI use cases in DHS's website, but it would be great if you could follow up and actually maybe use social media to point people to that. One of the things I'm always concerned about, with transparency of AI use

cases, is whether they're being explained to us by government, connecting us to the examples, because I think a lot of people are concerned about the flow, and would like to know how AI is making a difference there. You mentioned the concern about using technology. Earlier in the conference, we talked we heard from the FTC commissioner who mentioned that they banned Rite Aid from using facial recognition for five years, and a National Academy study that raised some real issues with potential civil liberties issues. We've seen, at many parts of our country now, facial recognition is been used in transit, the borders, both in commerce and in interactions with the government now, are there any conditions in which the DHS would consider putting a moratorium on the use of facial recognition, if you saw widespread issues with poor targeting of people, and the kinds of problems we've seen with predictive policing at the local level?

Robert Silvers
Thank you very much. First of all, just your first point, I really strongly agree that it's important we explain how we're using AI, certainly just for transparency, but also because a big part of this is going to be getting Americans to believe that AI is good for them, and building trust, because, if that collapses, a lot else will collapse with it in terms of the space that any of us have to use the technology. Part of that is just putting it out there, explaining it, and making it a little more tangible, because, let's be honest, a lot of these discussions can feel really up in the clouds to people who haven't been trained and educated in these specific issues, so I really do agree with the recommendation that we all explain our use better.

As to the use of facial recognition. It's really important to have very strong privacy and civil rights and civil liberties protections around that kind of technology. As a department, we do use facial recognition technology, for example, for traveler screening, and passage at airports, and the like. I will say, it's overwhelmingly popular with travelers, because it's fast, and it saves them from having to do things that create friction and cost them time. We bake in a lot of protections. There's automatic deletion of data. It's retained for very short periods, if at all, and kept only if needed for a specific investigation. It's subject to auditing and the like. And so, there is a strong range of guardrails to make sure that the use of these technologies, and the entrustment of people's biometric data, is not abused. We believe in the strength of those protections, and are constantly evaluating them and looking to see if anything does need to be strengthened, because, let's call a spade a spade, there is no question that facial recognition technology can be abused, in the wrong hands. It can be a tool for repression, and suppression of civil liberties, and the like. It also can have enormous efficiencies and benefits. The key in a democratic system like ours is to use it responsibly, use it in a limited way, and then always subject to safeguards that we're super transparent about, and can explain to the world, and then which are subjected to independent verification that we're actually following through on those commitments, and that's our approach.

Shane Tews
Undersecretary, thank you for spending your time with us today, and being our closing speaker of today's forum. So, please give him a round of applause.

Robert Silvers
Thank you, Shane. Thank you, everyone.